ABSTRACT

The present invention pertains to the field of electrical communication and computer technology, and more precisely, relates to cryptographic methods and devices for encryption of digital data. The method comprises forming an encryption key in the form of a set of subkeys, breaking down a data block into a number of subblocks $N \geq 2$, and alternate converting the subblocks by carrying out a dual-locus operation on a subblock and subkey. This method is characterised in that before carrying-out the dual-locus operation on the i-th subblock and subkey, a conversion operation depending on the j-th subblock is carried out on the subkey, where $j \neq i$. This method is also characterised in that the conversion operation depending on the j-th subblock is a permutation operation on the subkey bits depending on the j-th subblock. This method is further characterised in that the conversion operation depending on the j-th subblock is a cyclic offsetting operation on the subkey bits depending on the j-th subblock. The method is finally characterised in that the conversion operation depending on the j-th subblock is a substitution operation carried out on the subkey according to the j-th subblock.